EXHIBIT 12

DECLARATION OF STEPHEN M. BUNTING

I, STEPHEN M. BUNTING, DO HEREBY DECLARE:

1. My name is Stephen Michael Bunting. I am over the age of twenty-one (21), and I am competent to make this Declaration. I make this Declaration voluntarily and the facts stated herein are based on my personal knowledge and information.

2. Attached hereto as Exhibit "A" is a true and accurate copy of my Curriculum Vitae which truly and accurately represents my relevant employment history, training, experience, certifications, and expert-witness experience.

3. I currently work as Director of Services for SUMURI, LLC and as independent forensic consultant as owner of Bunting Digital Forensics, LLC. Prior to that, I was a police officer from 1980 until 2009 with the University of Delaware Police from which I retired as a Captain. During the last ten years with the University of Delaware Police, I was in charge of the digital forensics and cyber investigations unit, that I founded. From 2009 until early 2013, I was a Senior Forensic Consultant with Forward Discovery, LLC, which in late 2012 was acquired by Alvarez and Marsal (NY) where I was a manager in the digital forensics division. I founded Bunting Digital Forensics, LLC in early 2013.

4. I have taken hundreds of hours of training in digital forensics, network forensics, and cyber investigations. I have provided training in the same topic areas, from beginner to expert levels, to members of various local, state, and federal law enforcement agencies and private sector examiners. I have trained like personnel internationally in over twenty-one (21) different countries. I have provided training, as either a part-time employee or contractor, for Guidance Software, Magnet Forensics, MicroSystemation, A.B., Organization of American States, and the

U.S. Department of State Anti-Terrorism Assistance Program (Cyber Division). I have developed digital forensic or cyber training programs for several government and private entities.

5. I hold several industry-related certifications. I was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence for receiving the test score on my certification examinations. Among my varied certifications I am an EnCase Certified Examiner EnCE (Guidance Software), an AccessData Certified Examiner (ACE), Certified Computer Forensics Technician (HTCN), and a Certified XRY Instructor.

6. I am the principle author of *EnCase Computer Forensics - The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition,* the co-author of *Mastering Windows Network Forensics and Investigation, the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 2nd Edition*, and the co-author of *Mastering Windows Network Forensics and Investigation 2nd Edition, the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition* (all published by Wiley).

7. I have written numerous articles in the field of digital forensics over my career. Most recently, I published two articles regarding spoliation examinations in which several peer-to- peer cases on which I have consulted were referenced in a hypothetical context: *Forensic Analysis of Spoliation and Other Discovery Violations - Part 2 of a 2-Part Series - Windows Examinations* - eForensics Magazine - December 2016 *Forensic Analysis of Spoliation and Other Discovery Violations - Part 1 of 2-Part Series - Macintosh Examinations* - eForensics Magazine - October 2016

8. I have testified as a fact and expert witness numerous times in the field of computer forensics before state and federal courts in Delaware and New Jersey. I have submitted affidavits,

as an expert in digital forensics, on many matters in several states, including Delaware, Georgia, and South Carolina.

9. No court has ever refused nor has any attorney ever challenged to accept my testimony on the basis that I was not an expert or not qualified in the field of computer forensics.

10. As a digital forensics examiner I have acquired and examined hundreds of computer systems and mobile devices for various local, state, and federal agencies, in addition to scores of private clients. The types of cases or examinations include: homicide, child-exploitation, fraud, Medicaid fraud, unlawful intrusion into computer systems (hacking), intellectual property theft, research fraud, email forgery, criminal impersonation, forgery, sexual harassment, peer-to-peer, and spoliation. I have acquired computer systems of many types, including servers, virtual servers, desktops, and laptops. I have acquired hundreds of mobile devices (feature phones and smart phones), both logically and physically. I also have acquired smart phones using JTAG and chip-off techniques, both of which require disassembly and working with the printed circuit boards inside a smart phone.

11. I have considerable experience with network-related cases, such as unlawful intrusions and peer-to-peer cases. I have investigated or provided digital forensics support to several unlawful intrusion incidents in both a law enforcement and a private sector capacity.

12. In the past, I have consulted with Computer Forensics, LLC, in copyright infringement cases utilizing IPP's technology. I'm familiar with the technology that was used in those cases to detect the copyright infringement offenders.

13. As a police officer I received specialized training in conducting peer-to-peer investigations by S.A. Flint Waters with the Wyoming Internet Crimes Against Children (ICAC) Task Force. S.A. Waters developed the Wyoming Toolkit, a customized version of Phex, a peer-

to-peer client on the Gnutella network. I participated with members of the State of Delaware ICAC in this training program and afterwards in a task force conducting peer-to-peer investigations. Using the Wyoming Toolkit, we searched for child sexual exploitation images and movies on the peer-to-peer networks. When images were found, the software identified offending computers by their IP addresses.[1] The IP addresses hosting the illegal images are parsed by the toolkit using an IP geolocation database by which offending IP's are isolated or filtered to only those within our police jurisdiction. Once offending IP's were found in Delaware, we would request that the Attorney General's office submit subpoenas to the ISP (Internet Service Provider) for specific customer information and address of the offending IP address. As IP addresses are often time-specific, we submitted the exact date / time (along with time zone offset) for the offending IP address. The ISP would return to us the customer or subscriber information (name, address, account information, etc.) for the ISP in question. We would investigate further and obtain a search warrant for the premises at which the IP was hosted. The search warrant would permit us to seize all media and electronic devices capable of holding digital media, as we did not know specifically which device behind the router was the offending device. The IP address detected by the peer-to-

[1] A public or internet routable IP address is a router or computer's address on the internet at a specific time. IP addresses uniquely identify a computer, as no two computers can have the same exact public, internet routable, IP address at the same time. If the address is that of a router, the computer typically has a private address behind the router. In a typical home network, the ISP provides a 'box,' which is often both a modem and a router / firewall / DHCP server. The router has a public or internet facing IP address assigned to it. On the back side of the router, several devices (computers, smart phones, etc.) are connected using private addresses. Thus, several devices in a home network share the public internet routable address assigned to the ISP's box (router). Other computers on the internet, including peer- to-peer software, see and use the public facing IP address assigned to the customer's router. The router routes network traffic for specific devices on the private side or behind the router using a protocol called NAT (Network Address Translation), thus assuring network traffic is sent to the correct computer. IP addresses, as mentioned, are often time specific. These IP addresses are called dynamic IP addresses. They are assigned for certain periods of time, called leases. There is great variability in how often dynamic IP addresses change, but because they can and do change, the specific time of the offense is necessary to determine which subscriber was assigned a specific IP address at a specific time. ISP's maintain connection logs that record to whom a specific IP address is assigned and exactly when. By contrast, an IP address can be a fixed IP address. Even they can change and, as an investigator, you do not know which type a subscriber has and thus the exact time is always obtained and submitted to an ISP when requesting subscriber information.

peer software was the public facing internet addressable IP address of the router, which is associated with the subscriber and their residence and not to a specific computer in the residence. Because it was a criminal investigation, we requested that the subscriber not be notified of the subpoena so that digital evidence would not be destroyed. Thus, in nearly all cases, the offending subscribers were surprised by the execution of the search warrant. In all the times that we did so, not once did the IP address lead to an innocent person's residence. Rather, we always found evidence therein of child sexual exploitation media on the computer system(s) therein.

14. I have found that the Wyoming Toolkit was a most reliable tool for identifying the IP addresses for peer-to-peer clients that were hosting child sexual exploiting images and video.

15. Most recently, I tested the infringement detection software by a company called MaverickEye UB (MEU). This software and hardware platform is owned and run by GuardaLey, LTD ("GuardaLey"), a German company located in Eggenstein, Germany. It is my understanding that GuardaLey's system is substantially similar to another German company called IPP International UG ("IPP").

16. I constructed and then conducted a test to determine the accuracy of the GuardaLey's system as to its ability to detect an infringing party's IP address, identifying metadata (client software and version used by infringer), and identifying the known test files distributed on the torrent network. The manner in which GuardaLey's system works and the manner in which the software that I have used in my law enforcement capacity (Wyoming Toolkit) work to connect a peer-to- peer violation with an IP and subsequently with a subscriber are quite similar. In fact, in my opinion, GuardaLey's system is much better with greater integrity features. Further, my test confirmed that GuardaLey's system is accurate. My report illustrating this conclusion is attached hereto as Exhibit "B."

17. I have been retained by Strike 3 Holdings, LLC to provide digital forensic services and consulting in matters of copyright infringement. I am paid on an hourly basis by Strike 3 Holdings, LLC at the rate of $250 / hour for my digital forensics services.

18. I have read through the Honorable Judge Royce C. Lamberth's Memorandum Opinion ("DC Opinion") in the matter *Strike 3 Holdings, LLC v. John Doe subscriber assigned IP address 73.180.154.14*, No. CV 18-1425, (D.D.C. Nov. 16, 2018). The instant declaration specifically addresses the portion of the DC Opinion discussing the technology behind Strike 3 Holdings' case. And more specifically, the portion of the DC Opinion which states:

> Since Bittorrent masks users' identities, Strike 3 can only identify an infringing Internet protocol (IP) address, using geolocation technology to trace that address to a jurisdiction. This method is famously flawed: virtual private networks and onion routing spoof IP addresses (for good and ill); routers and other devices are unsecured; malware cracks passwords and opens backdoors; multiple people (family, roommates, guests, neighbors, etc.) share the same IP address; a geolocation service might randomly assign addresses to some general location if it cannot more specifically identify another.

STRIKE 3 HOLDINGS, LLC, Plaintiff, v. JOHN DOE subscriber assigned IP address 73.180.154.14, Defendant., No. CV 18-1425, 2018 WL 6027046, at *1 (D.D.C. Nov. 16, 2018).

19. Below, I address each of the foregoing issues in turn.

Virtual Private Networks and Onion Routing Spoofing of IP Addresses

20. Often times, in cases involving cybercrimes and IP addresses, defendants claim that their IP address was "spoofed." However, in cases involving detection systems that connect to peers using a TCP/IP connection, such as the Wyoming Toolkit, GuardaLey's system, or IPP's system, spoofing cannot be accomplished.

21. IP spoofing is typically used in DDOS (denial of service) attacks. Indeed, specially crafted network packets can be used to create denial of service attacks, but these packets are small and usually involve repeatedly sending the same small crafted packet over and over again, creating

a flood of messages that results in a denial of service attack. Creating a few small, specially crafted packets that are sent repeatedly is a completely different task than trying to do so for a BitTorrent stream, where tens of thousands of packets, mostly all of which are different, are involved.

22. With respect to spoofing in the BitTorrent context, in a practical sense, a very technically adept person would have to know a victim's IP address. This person would have to physically connect a computer into the same network segment as the intended victim in order to intercept the network traffic involved. Doing so would involve considerable knowledge and skills, in and of itself, and could involve illegal access to a building or ISP network equipment. The person would need to have the file in question on their computer, be sharing it using BitTorrent software, and have some software or code capable of or rewriting tens of thousands of BitTorrent packets on the fly, as any delay could cause a time-out. While many things are theoretically possible, I am unaware of any such software being available. Such an endeavor would involve tremendous effort and resources. In addition, the person would have to know that a particular file was being monitored for copyright infringement downloading. And finally, such a person would have to have a very strong motivation to undertake such a task and to target a particular person and/or IP address. Considering all that would be involved in such an endeavor, it is so unlikely to occur as to be nearly impossible.

23. Often IP spoofing, as described above, is interpreted or confused by many, including Google's search engine, with IP address hiding. If you search for "IP spoofing software," you will find most of the search results will involve VPN (Virtual Private Network) software. VPN software allows the user of a computer to create an encrypted tunnel to a VPN server from which the internet traffic emerges unencrypted, provided of course it was unencrypted to begin with. The VPN server's internet facing IP address becomes the user's public internet-

routable IP address. It acts as a proxy and becomes the user's frontend IP address on the internet. VPN's are intended for privacy of a user's internet traffic and also for protecting the identity of a user's true IP address (the IP address which their ISP has assigned to them). If an infringer uses a VPN to engage in BitTorrent file sharing, other peers within the swarm will be able to identify the infringer by the infringer's public facing internet routable IP address which would the VPN's IP address. In other words, when a VPN is being used, other peers can only trace the connection to the front-end or public-facing, internet routable IP address – which would be the VPN IP address. To obtain the true IP address of the user behind the VPN, one would have to contact the VPN owner or manager. If the VPN owner maintain logs, and many intentionally do not, the connection to the source can then be identified through the subpoena process.

24. In the past, I actually conducted a test on this exact VPN issue. Indeed, earlier this year, when I tested Guardaley's system, I also tested this VPN theory. To do so, I configured one test laptop (MacBook Pro – High Sierra) with a VPN service. With the VPN enabled, I launched Transmission (a popular BitTorrent client) and shared four separate test files. I noted the public, internet-routable, frontend VPN IP address in use by the test laptop. After running this BitTorrent configuration overnight using the VPN service, GuardaLey reported to me that their system captured and downloaded the test files from the IP address that I had recorded for the test laptop. It was, as expected, the IP address of the VPN server. Thus, a test of the scenario, establishes that the VPN IP address, and not my true ISP's IP address was being made public via the BitTorrent network.

Unsecured Routers and Other Devices

25. The DC Opinion also lists concerns about unsecured routers and devices.

26. During my time at Bunting Digital Forensics, LLC, I was involved in a case where the owner of the computer and charged party was professing his innocence, claiming someone else must have used his wireless network, citing a neighbor who reportedly engages in photography of a questionable nature. However, the evidence on his computer suggested otherwise. The software used by the investigators detected the name and version of the peer-to-peer software client involved, which happened to match the one found on his machine. Further, the same exact images detected by the investigative software were found on his machine. His claims were without merit and in direct contradiction to the overwhelming digital evidence found on his computer.

27. Unsecured wireless routers in homes used to be commonplace 15 years ago. In recent years, however, Internet Service Providers (ISP's) have undertaken great effort to provide and deploy secured wireless systems. Most "internet interface boxes" (combination modem / router / firewall / DHCP server) which are rented to subscribers are preconfigured to operate with WPA2 security with a complex password already set. These devices are secure out of the box with strong encryption and complex passwords that are lengthy alpha numeric passphrases. Thus, valid claims of compromised home wireless systems today are, in my experience, rare compared to 15 years ago.

Malware Cracks Passwords and Open Backdoors

28. The DC Opinion states, that "malware cracks passwords and opens backdoors." However, I have never heard of or encountered malware which accesses a user's computer, automatically downloads and installs a BitTorrent client, and then proceeds to download .torrent files correlating to several of Plaintiff's works over the course of several months.

Multiple People Share the Same IP Address

29. Although there may be several household members who access the internet with the same router, learning the identity of the subscriber to an IP address user in connection with commission of a crime is instrumental, necessary, and the only means of learning the perpetrator's true identity – even if the subscriber is not the perpetrator.

30. And, in my experience, the IP address's subscriber, or a family member thereof, is likely the offending party.

Geolocation Technology

31. Lastly, the DC Opinion states, "a geolocation service might randomly assign addresses to some general location if it cannot more specifically identify another."

32. Geolocation services are used to approximate locations of IP addresses. Such geolocation services are often used as a tool in e-commerce fraud prevention measures. Further, the Wyoming Tool Kit that I used as a law enforcement officer to identify offenders distributing sexual exploitive images of children using peer-to-peer software, used commercial geolocation services to obtain the approximate location of IP addresses for purposes of assigning IP addresses to various law enforcement jurisdictions. Geolocation databases are not used to determining the exact address of a subscriber of an IP address for purposes of executing a search warrant. Rather, to determine an IP address subscriber's physical address on which to execute a search warrant, law enforcement relies on a subpoena that is served upon the ISP. When law enforcement uses this technology and methodology to identify and arrest those creating and exchanging sexually exploitive images of children, they are applauded for their efforts. Similarly, Strike 3 Holdings, LLC uses geolocation services to determine an approximate location of an IP address so as to identify a court with jurisdiction in that region. Once that court issues a subpoena, the exact name

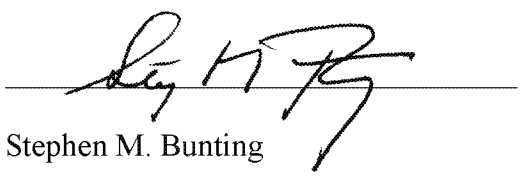
and specific physical address of the party responsible for the offending IP is identified. Strike 3 Holdings, LLC is, thus, using a process very much like that used by law enforcement.

FURTHER DECLARANT SAYETH NAUGHT

DECLARATION

PURSUANT TO 28 U.S.C SS 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed December 11, 2018.



Stephen M. Bunting